Windows at Fermilab

Windows 2000/XP Desktop Baseline Security Configuration

Introduction

This guide provides FNAL Windows desktop administrators guidance regarding the proper configuration of the Microsoft Windows 2000 Professional and XP Professional operating system security settings in accordance with Fermi National Accelerator Laboratory security requirements and guidelines.

The Fermi National Accelerator Laboratory Security Baseline configuration settings represent industry best practices for securing Windows 2000 and XP desktop computers, based on recommendations from several sources including Microsoft, the SANS Institute, the National Security Agency (NSA), and the Center for Internet Security (CIS). The settings were reviewed and modified by the Windows Policy Committee for compliance with the Fermi National Accelerator Laboratory operational environment.

This document presents the minimum level of security settings along with “Good Admin Practice”. As such, all of the settings unless noted as “Good Admin Practice” are mandatory requirements. The mandatory system requirements are standard settings for systems that participate in the FNAL Windows Active Directory infrastructure. This document does not attempt to cover additional desktop settings that may be enforced for an individual OU within the Active Directory domain.

Purpose

The settings discussed in this guide are intended to minimize the exposure of a Windows 2000 Professional or XP Professional desktop to known vulnerabilities.

Scope

This document discusses the configuration of systems installed with Microsoft Windows 2000 Professional or XP Professional systems covered under the lab Enterprise Agreement. The recommendations contained herein do not apply to Windows OSes not covered under the Approved OS page found on the Windows Policy Committee website.

Intended Audience

This document is intended for system administrators responsible for the security of Microsoft Windows 2000 Professional and XP desktop systems at Fermi National Accelerator Laboratory. It assumes that the reader has knowledge of the operating systems and is familiar with common computer terminology and common administrative tasks.

Physical Security

Desktop systems must be physically secured to ensure that unauthorized individuals do not gain access to the systems. Security cables should be used to prevent theft. Password locked screen savers are to be used to prevent unauthorized access.

Secure Installation

Prior to placing a Windows desktop on the FNAL network, the system administrator must ensure that the patches required by Computer Security are installed. A list of these patches are available on the Computing Division Security website. Required patches are available for download from the Computing Division Windows software distribution server.

In addition to critical patches, desktops must have anti-virus software installed and operating as defined in the Fermilab Antivirus baseline before[j1] connecting to the network. Once on the network the desktop will be updated with the newest signature file from one of the central anti-virus servers.

NTFS

Microsoft Windows 2000 Professional and XP Professional systems on the FNAL network must be configured with the NTFS file system.

Domain Membership

Microsoft Windows 2000 Professional and XP Professional systems should participate in the FNAL Active Directory domain fermi.win.fnal.gov. Systems placed into the domain have additional policies applied automatically to meet the security guidelines. Systems not in the domain[j2] must document and demonstrate they meet the minimum level defined in this baseline..

Kerberos/NTLMv2

Microsoft Windows 2000 Professional and XP Professional desktops must be configured to only allow Kerberos/NTLMv2 authentication. By default, domain systems communicate via Kerberos. Non-domain systems can only authenticate via Microsoft NTLM authentication and are required by the FNAL security policy to only use NTLMv2.

Password Policy

Microsoft Windows 2000 Professional and XP Professional desktops local password policy must match the FNAL Active Directory domain password policy.
The domain password policy is found on the Windows Policy Committee website.

Banner

Microsoft Windows 2000 Professional and XP Professional desktops must display the DOE login banner[j3] .

SMS

Microsoft Windows 2000 Professional and XP Professional desktops must be configured to use either the approved Divisional or Central SMS server. The site SMS server is used for software and hardware inventory, software application and active patching of systems.

WUS

Microsoft Windows 2000 Professional and XP Professional desktops must be configured to use the approved Divisional or site WUS server. The site WUS server is used for verifying Computer Security required patches are applied to a system.

Audit Policies

Microsoft Windows 2000 Professional and XP Professional desktops must be configured with proper auditing settings. In addition to helping track software problems they are crucial in

diagnosing security incidents. A listing of proper audit settings is available on the Windows Policy website[j4] .

Restrict Anonymous Access
Best Practice:
Microsoft Windows 2000 Professional and XP Professional desktops should be configured to restrict anonymous enumeration of SAM accounts and shares. The current level supported by the FNAL Active Directory domain is 1. System Administrators are encouraged to set this to a higher level whenever possible.

IPSEC/Firewall
Best Practice:
It is strongly recommended that Microsoft Windows 2000 Professional and XP Professional systems be configured with a personal firewall. To use DHCP, any firewall configuration will require the ability to 'ping' (ICMP) the computer from at least other FNAL nodes. It is also strongly recommended that logging of permit/deny events be enabled where possible. System Administrators are strongly encouraged to make use of the built-in Microsoft firewall in XP, IPSEC filters in Windows 2000 System, or 3rd. party Desktop Firewall software (.e.g. McAfee, Symantec, Zone Alarm).

Network Access
Best practice:
Microsoft Windows 2000 Professional and XP Professional desktops must be configured to restrict access from the network. By default the FNAL Active Directory domain policy is to only allow domain members, computers and domain administrators' remote access to desktops. Local user accounts cannot be used to remotely access resources as stated in the FNAL Strong Authentication policy.

Non-Domain Recommendations
In addition to domain policies the following are Best Practice recommendations and as of yet are not domain policies.

File Sharing
Best Practice:
By default, desktop systems should not be configured for file serving.
This is served by Divisional or central file servers.

Printer Sharing
Best Practice:
By default, desktop systems should not be configured for printer sharing. This is better served by Divisional or central print servers.

Web Services
Best Practice:
By default, desktop systems should not be configured to run web services due to the demands to ensure a secure operating environment. Web publishing should be performed on the Divisional or central web servers. Systems that need to run Web services with offsite access require an exemption from the FNAL Computer Security Team. This goes for Web services offered on any

port, not just the standard HTTP/HTTPS ports.

Instant Messaging

Best Practice:
The onsite jabber.fnal.gov server should be used. Gaim is the FNAL supported client. Use of other IM software such as AOL or MSN is not suggested as it is often not encrypted and allows for possible sensitive data passing though offsite servers. In addition, these common IM services are a target for scams, trojans and viruses.

Use of Administrator Privileges

Best Practice:
Users of Microsoft Windows 2000 Professional and XP Professional desktops should not use an account with administrative rights for daily work. Privileges should be elevated only when necessary and for a short period of time.

[j5]

References

This section provides a list of references used in developing this document.

1. FNAL Windows Policy Committee website:
   http://plone3.fnal.gov/WinPol/

2. FNAL SMS website:
   http://www-win2k.fnal.gov/private/sms/

3. FNAL SUS website:
   http://sus.fnal.gov

4. FNAL Computer Security Website:
   http://security.fnal.gov

5. FNAL Windows Distribution Server:
   http://pseekits.fnal.gov

6. The Center for Internet Security Benchmark tools
   http://www.cisecurity.org/bench_win2000.html

7. NSA Guide to Securing Microsoft Windows XP
   http://www.nsa.gov/snac/os/winxp/winxp.pdf

8. Microsoft Windows XP Security Settings
   http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_secsettop

~~7.~~9. DOE G 205.3-1, *Password Guide*.
   https://www.directives.doe.gov/pdfs/doe/doetext/restrict/neword/205/g2053-1.pdf

~~8.~~10. DOE N 205.3, *Password Generation, Protection and Use*
   https://www.directives.doe.gov/pdfs/doe/doetext/restrict/neword/205/n2053.pdf

[j1]Isn't this supposed to be defined in the baseline for frequency/updates –OR- in a more generic AV implementation document???
[j2]Is this true???
[j3]URL pointer??
[j4]URL pointer??
[j5]A complete listing of all the Domain policies should be listed (logon over network, etc.) or at least a pointer to the complete listing so non-Domain members can adhere to the baseline easily